Option Finance

► 23 avril 2024 - 09:06

Loi Lopmi : un an après, une mise en application difficile

Voilà désormais un an que l'article L.12-10-1 a été introduit dans le Code des assurances. Retour d'expérience sur ce texte qui conditionne la mobilisation des garanties d'assurance en cas d'incident de type attaque informatique au dépôt d'une plainte pénale dans un délai de soixante-douze heures.

Eleonora Sorribes, avocate associée, et Maxime Ramos-Guerrero, avocat, **LPA-CGR**

Le texte de l'article L.12-10-1 du Code des assurances, issu de la loi de programmation du ministère de l'Intérieur n°2032-22 du 14 décembre 2022, avait, au moment de son adoption, donné lieu à de nombreux débats, se focalisant notamment sur l'assurabilité du paiement des rançons, la nécessité de favoriser une réponse pénale adaptée, et un marché de l'assurance cyber encore peu développé en dehors des grands groupes. Il avait surtout donné lieu à une certaine incompréhension, le texte recélant nombre d'incohérences et de difficultés d'interprétation.

Nous nous étions livrés, dans ces mêmes pages, à une explication de texte dont la conclusion jugeait l'article L.12-10-1 du Code des assurances inadapté, insusceptible de remplir ses objectifs, et posant plus de questions qu'il n'apportait de réponses

Depuis l'entrée en vigueur du texte le 24 avril 2023, nous avons pu éprouver à travers différents sinistres les nombreuses difficultés de mise en œuvre auxquelles sont confrontés les assureurs, mais surtout les assurés, qui se sont vus imposer une obligation supplémentaire à respecter dans un délai strict et dans un contexte d'attaque informatique dont la gestion est particulièrement exigeante. Après un an, un premier bilan s'impose, les difficultés d'application du texte n'ayant pas manqué.

1- Un texte encore méconnu

Un premier constat s'impose, le texte de l'article L.12-10-1 est encore largement méconnu, même des entreprises assurées. En effet, le texte n'a pas fait l'objet, de la part des pouvoirs publics, d'une médiatisation particulière, alors même qu'il a des conséquences radicales pour les entreprises bénéficiant d'un contrat d'assurance. On rappelle que la sanction en cas d'irrespect est l'impossibilité de voir jouer les garanties de la police et donc de percevoir une quelconque indemnisation.

Les entreprises, face à un risque persistant (le risque cyber est considéré comme le risque le plus important par les conseils d'administration), se retrouvent ainsi dépourvues d'indemnisation dès lors qu'elles n'ont pas déposé plainte dans les

soixante-douze heures suivant la constatation d'un sinistre susceptible de constituer une des infractions d'atteinte à un système de traitement automatisé de données (atteintes au STAD) prévues aux articles 323-1 à 323-3-1 du Code pénal.

Sur ce point, et quand bien même le texte serait connu, il paraît particulièrement délicat de conclure, face à la constatation d'un sinistre, qu'il relève ou non d'une des infractions d'atteintes au STAD prévues par le Code pénal. Il s'agit en effet d'infractions dont les éléments matériels sont particulièrement techniques, tout à fait méconnus du grand public.

Face à cette méconnaissance, saluons les efforts pédagogiques importants déployés par les courtiers et compagnies d'assurance pour informer le plus largement les assurés. On notera par exemple que la plupart des courtiers et compagnies rappellent et insistent clairement par écrit, au moment de la déclaration de sinistre, sur l'existence de cette obligation légale afin que l'assuré puisse la respecter.

Reste le cas où la déclaration de sinistre interviendrait plus de soixante-douze heures après la constatation par l'assuré de la survenance du sinistre cyber et que la situation ne pourrait être régularisée compte tenu de l'expiration du délai légal.

2- Les difficultés quant au champ d'application matériel

Comme évoqué précédemment, la question de la méconnaissance du texte n'est pas le seul obstacle. Il existe en effet des situations dans lesquelles la question de l'applicabilité de l'article L.12-10-1 du Code des assurances se pose avec acuité. Dans le cadre d'une attaque par rançongiciel, il sera aisé de conclure à l'applicabilité du texte, tant il est évident qu'un tel sinistre est constitutif d'une des infractions d'atteinte à un STAD (l'assuré est dans l'incapacité matérielle d'accéder à ses données).

Cela sera en revanche beaucoup moins évident lorsque l'on est confronté à des situations s'éloignant d'un cas classique d'attaque par cryptolocker. Ainsi des situations où l'assuré suspecte une compromission de son système d'information mais sans pouvoir le confirmer techniquement, ne permettant pas de conclure à l'existence d'une telle atteinte au STAD. On pense notamment aux situations de fraudes (par exemple au faux RIB), ou d'attaques de type man-in-the-middle.

Dans certains cas, seules des investigations forensiques poussées ont permis de conclure à l'existence d'une compromission du système d'information de l'entreprise cible et donc à l'applicabilité de l'article L.12-10-1 du Code des assurances. En pareille hypothèse, il serait légitime de considérer que le délai de soixante-douze heures ne commence à courir qu'à l'issue des investigations techniques ayant pu conclure à la réalité de l'atteinte au STAD. Cette question ne trouve toutefois pas de réponse à l'heure actuelle et nous recommandons donc, par précaution, de procéder à un dépôt de plainte dans des situations où une atteinte au STAD ne serait que suspectée, quitte à ce que cette plainte soit retirée dans un second temps.

3- La difficulté à apprécier le point de départ du délai de soixante-douze heures

Faute de précision dans le texte, les assurés et compagnies se trouvent souvent démunis pour apprécier le point de départ du délai de soixante-douze heures. Selon l'article L.12-10-1 du Code des assurances, ce délai commence à courir « après la connaissance de l'atteinte par la victime ». Or, il paraît délicat de déterminer le moment où la victime a effectivement eu « connaissance de l'atteinte ». Il semble qu'à ce stade il s'agisse d'un point de départ subjectif, les uns pouvant considérer, dans une situation particulière, que l'assuré avait une connaissance suffisante, tandis que d'autres considérant qu'il n'avait pas à sa disposition l'ensemble des informations techniques suffisantes.

Sur ce point, nous raisonnons par syllogisme, et appliquons les règles relatives aux

violations de données à caractère personnel et les lignes directrices publiées par le Comité européen de la protection des données (CEPD) qui précisent « qu'un responsable de traitement devrait être considéré comme ayant pris "connaissance" lorsqu'il est raisonnablement certain qu'un incident de sécurité s'est produit et que cet incident a compromis des données à caractère personnel »

Ainsi, selon nous, un assuré ne saurait être considéré comme ayant eu connaissance d'une atteinte, selon les circonstances, sans qu'il ait pu mettre en œuvre des investigations techniques raisonnables. Évidemment, il pourrait être reproché à un assuré de n'avoir pas mis en œuvre une telle enquête alors qu'une atteinte au STAD pouvait raisonnablement être suspectée.

Il est à noter que, dans certaines situations, il pourra être considéré que l'assuré a eu une connaissance immédiate de l'atteinte. C'est notamment le cas dans des situations d'attaques par cryptolocker où la simple constatation d'un chiffrement suffit à faire partir le délai de soixante-douze heures.

4- Les difficultés quant au champ d'application territorial

Nous avions déjà pu pressentir de telles difficultés dans le cas de polices d'assurance ayant un champ d'application territorial sur le monde entier . Celles-ci ont pu se révéler concrètement dans des situations d'attaques informatiques concernant plusieurs personnes morales, membres d'un même groupe de sociétés, mais basées dans plusieurs pays. De tels sinistres sont rendus possibles par l'imbrication des systèmes d'information des différentes entités ainsi regroupées.

Dans de telles situations, une lecture littérale de l'article L.12-10-1 du Code des assurances pousse à conclure à la nécessité de déposer une plainte pénale dans l'ensemble des pays dans lesquels une des entreprises du groupe, couverte par le contrat d'assurance de droit français et souhaitant en bénéficier, a été impactée.

Les autorités de poursuites françaises n'ont en effet aucune compétence pour intervenir dans le cadre d'une attaque affectant une entreprise basée à l'étranger en application des articles 113-2 à 113-14 du Code pénal. En particulier, si la victime n'est pas française et aucun élément ne permet de considérer que l'infraction a été commise sur le territoire français.

Cette constatation n'est évidemment pas sans conséquences, les différentes personnes morales ayant la qualité d'assuré devant en effet, chacune, déposer sa propre plainte, dans le pays dans lequel elles ont leur siège, sans pouvoir bénéficier d'un unique dépôt, qui serait effectué en France par la société mère, qui est généralement la société souscriptrice.

5- La difficulté concrète à déposer plainte

Ces développements ressortent d'un simple constat : dans nombre de situations, les assurés ont pu être confrontés à un refus des effectifs de police ou de gendarmerie de recevoir leur plainte, et ce quand bien même, on le rappelle, un policier ou un gendarme a en principe l'obligation de recevoir l'ensemble des plaintes qui lui sont rapportées, étant de la seule responsabilité du procureur de la République de trancher sur les suites à donner. Bien souvent, ce refus de plainte est lié à une simple méconnaissance du texte de l'article L. 12-10-1 du Code des assurances mais plus encore, et c'est ce qui est inquiétant, des articles 323-1 à 323-3-1 du Code pénal.

Les assurés souhaitant déposer plainte en commissariat ou en gendarmerie ont pu également se voir rétorquer qu'il leur était nécessaire de procéder à un dépôt de plainte en ligne via la plate-forme Thésée. Pour rappel, à ce jour, la plate-forme Thésée permet de déposer une plainte en ligne mais uniquement pour les victimes ou témoins particuliers, ce qui exclut les professionnels, et pour des infractions spécifiques (piratage

de messagerie informatique, chantage en ligne, escroquerie, etc.). Une telle plainte en ligne n'est pas adaptée pour les assurés soumis à l'article L.12-10-1 du Code des assurances qui exclut les particuliers de son champ d'application. Nous rappelons encore que le dépôt d'une pré-plainte en ligne ne constitue pas une plainte pénale, et est donc insusceptible de remplir la condition fixée à l'article L.12-10-1 du Code des assurances.

La solution la plus simple et rapide reste pour les entreprises l'envoi d'un courrier recommandé avec accusé de réception au procureur de la République compétent (sur ce point la section J3 du parquet près le Tribunal judiciaire de Paris a une compétence nationale) qui peut être effectué directement en ligne via le site internet de La Poste

Reste encore la question des informations qui doivent être contenues dans cette plainte. Sur ce point, dans le silence du texte, nous suggérons une approche minimaliste en se contentant d'une description succincte des faits de l'espèce, avec les quelques informations essentielles. L'assuré aura par la suite le loisir de compléter sa plainte, notamment lorsqu'il disposera d'éléments techniques complémentaires (par exemple, après réception d'un rapport d'expertise forensique).

6- Conclusion : des incertitudes persistantes et une jurisprudence qui se fait attendre

Ainsi, la mise en œuvre de l'article L.12-10-1 du Code des assurances demeure aujourd'hui délicate et les assureurs comme les entreprises assurées sont parfois dépourvus face à des situations complexes qui n'avaient manifestement pas été anticipées par le législateur. Le bilan est donc mitigé. Faute de clarté dans l'interprétation, l'application de ce nouveau texte se fait souvent dans la confusion, et il n'existe pas, à notre connaissance, de pratique de marché établie. Cela donne nécessairement lieu à une insécurité juridique et à des interprétations péremptoires. Aucune jurisprudence n'étant encore venue éclairer les praticiens. Le contentieux se fait attendre et il y a tout lieu de penser qu'il mettra encore du temps avant de survenir.

Pour ajouter à la confusion, les compagnies n'ont à ce jour aucune visibilité sur les sanctions qu'elles encourraient si elles décidaient d'indemniser les conséquences d'un incident informatique alors qu'il existe un doute sur la date de connaissance de l'atteinte au STAD (et donc une incertitude sur le respect par l'assuré du délai fixé par l'article L.12-10-1 du Code des assurances). Ou plus encore que le délai de soixante-douze heures n'ait pas été respecté et que les compagnies indemnisent, à titre commercial néanmoins, du fait de la bonne foi de l'assuré.

Face à ces incertitudes, certaines entreprises et compagnies d'assurance réflechissent à soumettre leurs contrats d'assurance à un droit étranger afin d'échapper au dispositif contraignant de la loi LOPMI. Espérons que cette confusion pourra finalement être dissipée, mais probablement pas avant un contentieux. Il est toutefois difficilement admissible que des entreprises assurées se retrouvent potentiellement pénalisées du fait des ambiguïtés de la loi, alors même que les entreprises non assurées n'ont aucune obligation de reporter une attaque informatique.

« Loi Lopmi : le mieux est l'ennemi du bien » La Tribune de l'assurance, 4 avril 2023, E. Sorribes, M. Ramos-Guerrero, M. Hassan

Rapport de situation en France – Risques et résilience en période de changement, Beazley, janvier 2024 : https://www.beazley.com/globalassets/2024-01/240113_france-report_final.pdf

Article 33 du règlement général sur la protection des données 2013/679 du 27 avril 2016

EDPB – Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 du 6 février 2018

« Loi Lopmi : le mieux est l'ennemi du bien », La Tribune de l'assurance, 4 avril 2023, E.